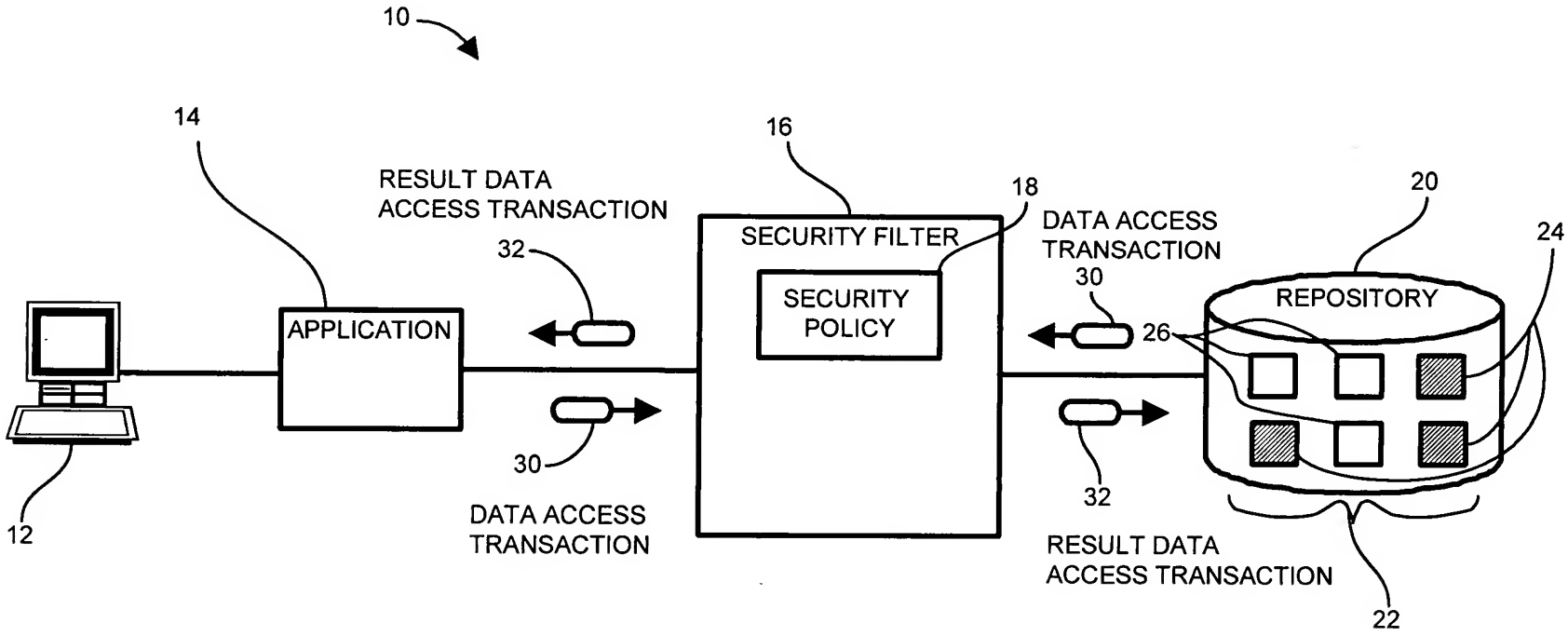

10
14
16
18
20
24
RESULT DATA
ACCESS TRANSACTION
SECURITY FILTER
DATA ACCESS
TRANSACTION
32
SECURITY
POLICY
30
REPOSITORY
APPLICATION
26
30
32
12
DATA ACCESS
TRANSACTION
RESULT DATA
ACCESS TRANSACTION
22

Fig. 1

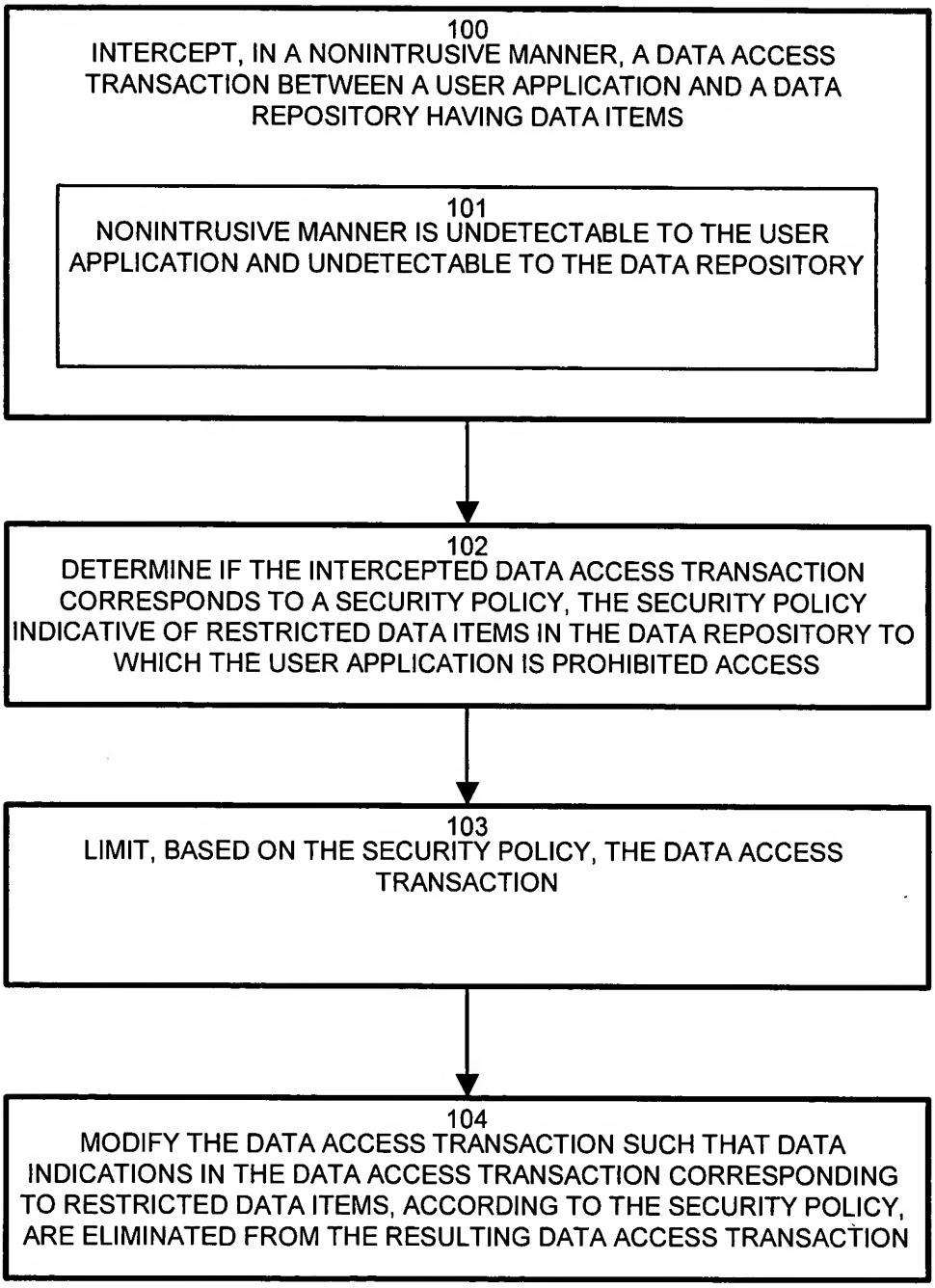

100
INTERCEPT, IN A NONINTRUSIVE MANNER, A DATA ACCESS TRANSACTION BETWEEN A USER APPLICATION AND A DATA REPOSITORY HAVING DATA ITEMS
101
NONINTRUSIVE MANNER IS UNDETECTABLE TO THE USER APPLICATION AND UNDETECTABLE TO THE DATA REPOSITORY
102
DETERMINE IF THE INTERCEPTED DATA ACCESS TRANSACTION CORRESPONDS TO A SECURITY POLICY, THE SECURITY POLICY INDICATIVE OF RESTRICTED DATA ITEMS IN THE DATA REPOSITORY TO WHICH THE USER APPLICATION IS PROHIBITED ACCESS
103
LIMIT, BASED ON THE SECURITY POLICY, THE DATA ACCESS TRANSACTION
104
MODIFY THE DATA ACCESS TRANSACTION SUCH THAT DATA INDICATIONS IN THE DATA ACCESS TRANSACTION CORRESPONDING TO RESTRICTED DATA ITEMS, ACCORDING TO THE SECURITY POLICY, ARE ELIMINATED FROM THE RESULTING DATA ACCESS TRANSACTION

Fig. 2

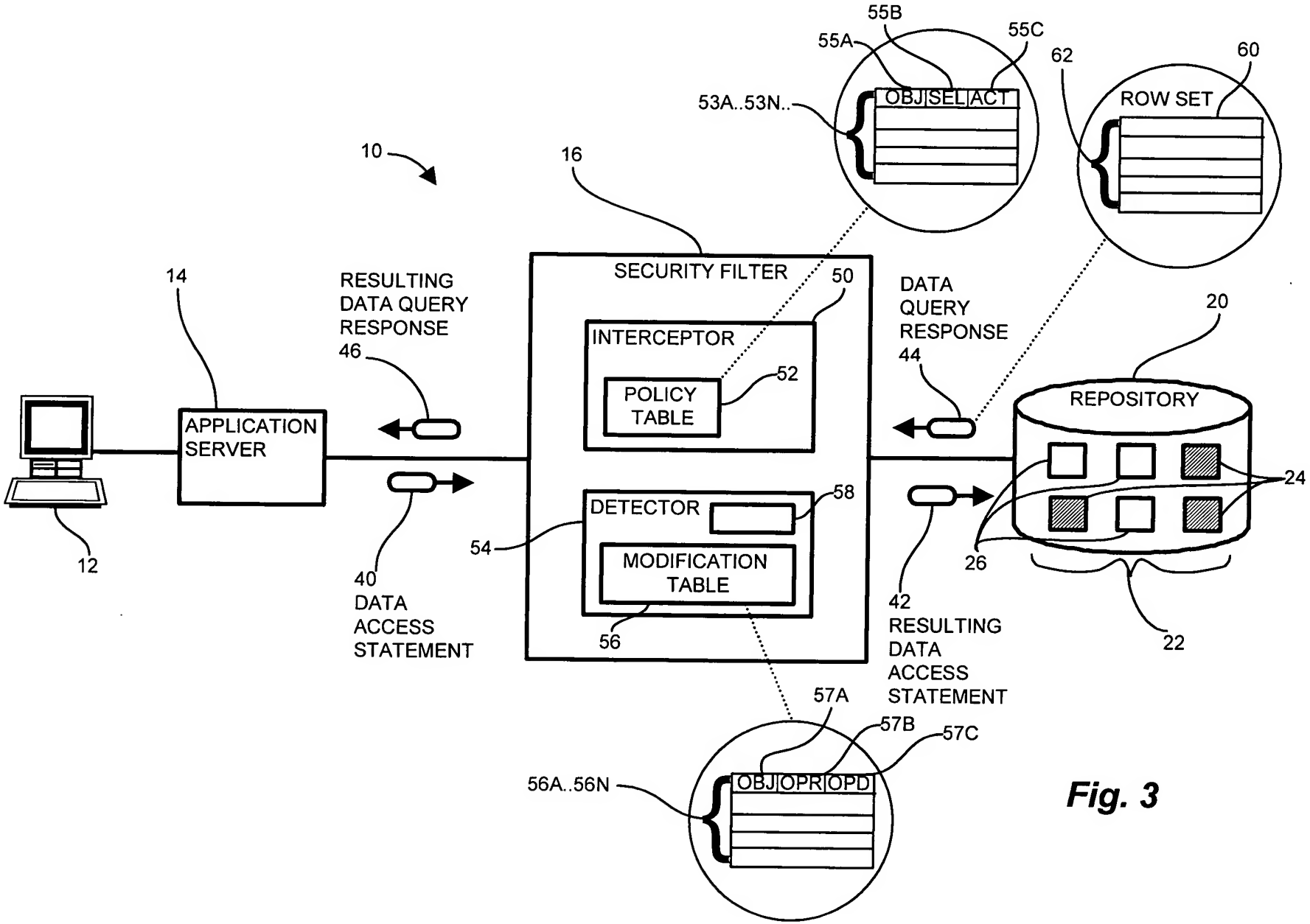

10
12
14
16
SECURITY FILTER
50
INTERCEPTOR
52
POLICY TABLE
DETECTOR
58
MODIFICATION TABLE
54
56
APPLICATION SERVER
RESULTING DATA QUERY RESPONSE
46
40
DATA ACCESS STATEMENT
DATA QUERY RESPONSE
44
42
RESULTING DATA ACCESS STATEMENT
REPOSITORY
20
24
26
22
55A
55B
55C
OBJ SEL ACT
53A..53N..
62
ROW SET
60
57A
57B
57C
OBJ OPR OPD
56A..56N

Fig. 3

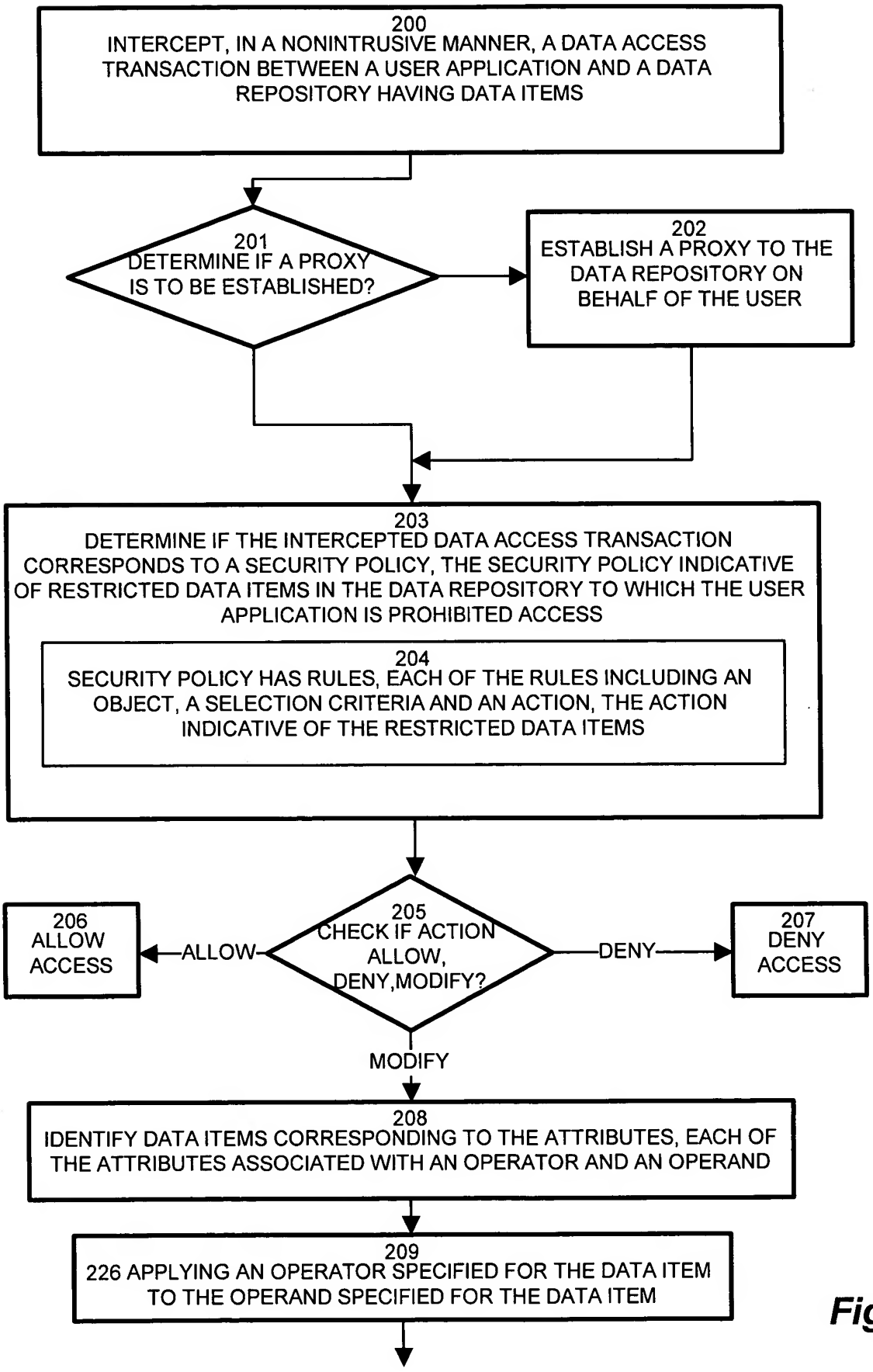

200
INTERCEPT, IN A NONINTRUSIVE MANNER, A DATA ACCESS TRANSACTION BETWEEN A USER APPLICATION AND A DATA REPOSITORY HAVING DATA ITEMS
201
DETERMINE IF A PROXY IS TO BE ESTABLISHED?
202
ESTABLISH A PROXY TO THE DATA REPOSITORY ON BEHALF OF THE USER
203
DETERMINE IF THE INTERCEPTED DATA ACCESS TRANSACTION CORRESPONDS TO A SECURITY POLICY, THE SECURITY POLICY INDICATIVE OF RESTRICTED DATA ITEMS IN THE DATA REPOSITORY TO WHICH THE USER APPLICATION IS PROHIBITED ACCESS
204
SECURITY POLICY HAS RULES, EACH OF THE RULES INCLUDING AN OBJECT, A SELECTION CRITERIA AND AN ACTION, THE ACTION INDICATIVE OF THE RESTRICTED DATA ITEMS
205
CHECK IF ACTION ALLOW, DENY,MODIFY?
ALLOW
206
ALLOW ACCESS
DENY
207
DENY ACCESS
MODIFY
208
IDENTIFY DATA ITEMS CORRESPONDING TO THE ATTRIBUTES, EACH OF THE ATTRIBUTES ASSOCIATED WITH AN OPERATOR AND AN OPERAND
209
226 APPLYING AN OPERATOR SPECIFIED FOR THE DATA ITEM TO THE OPERAND SPECIFIED FOR THE DATA ITEM

Fig. 4

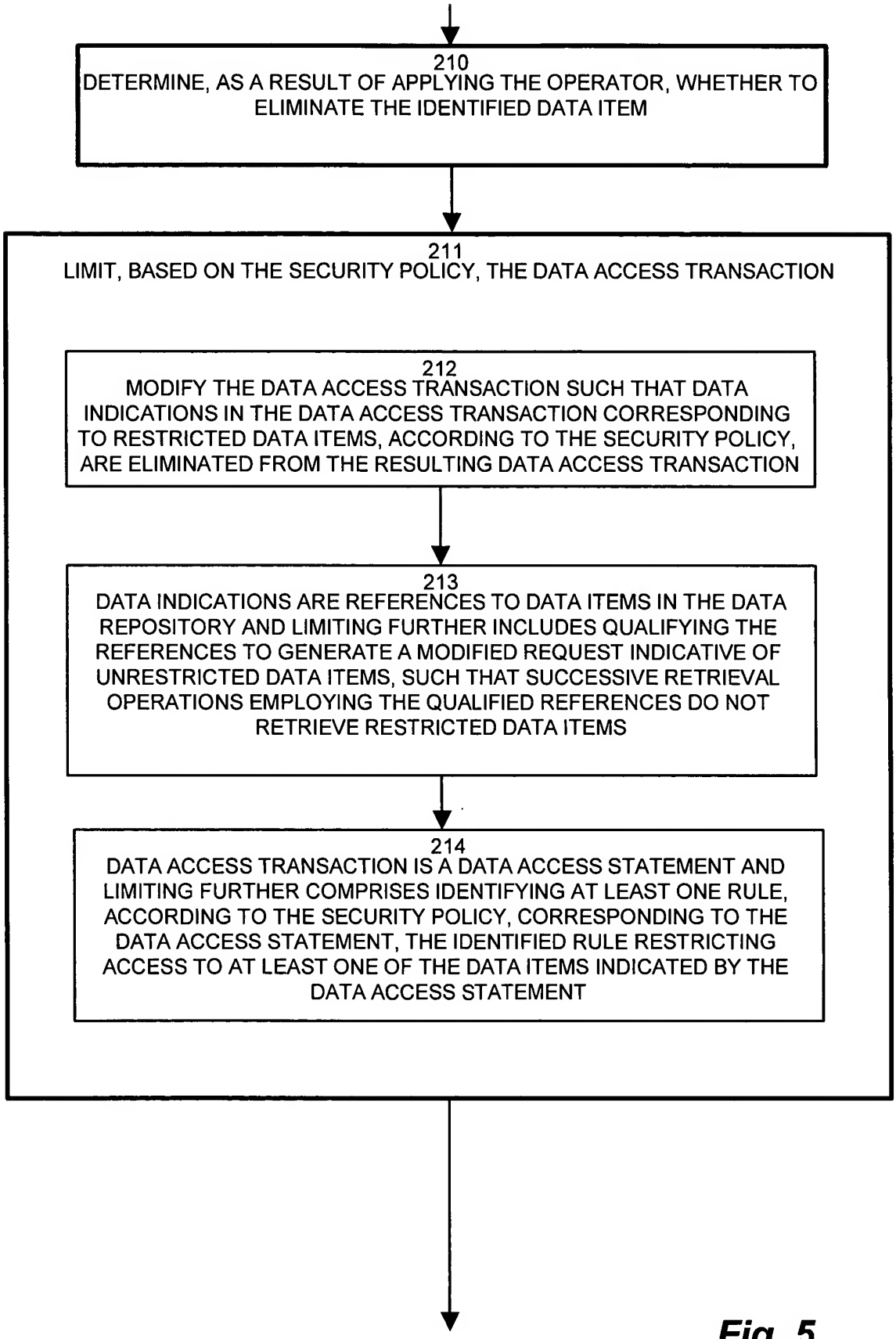

210
DETERMINE, AS A RESULT OF APPLYING THE OPERATOR, WHETHER TO ELIMINATE THE IDENTIFIED DATA ITEM
211
LIMIT, BASED ON THE SECURITY POLICY, THE DATA ACCESS TRANSACTION
212
MODIFY THE DATA ACCESS TRANSACTION SUCH THAT DATA INDICATIONS IN THE DATA ACCESS TRANSACTION CORRESPONDING TO RESTRICTED DATA ITEMS, ACCORDING TO THE SECURITY POLICY, ARE ELIMINATED FROM THE RESULTING DATA ACCESS TRANSACTION
213
DATA INDICATIONS ARE REFERENCES TO DATA ITEMS IN THE DATA REPOSITORY AND LIMITING FURTHER INCLUDES QUALIFYING THE REFERENCES TO GENERATE A MODIFIED REQUEST INDICATIVE OF UNRESTRICTED DATA ITEMS, SUCH THAT SUCCESSIVE RETRIEVAL OPERATIONS EMPLOYING THE QUALIFIED REFERENCES DO NOT RETRIEVE RESTRICTED DATA ITEMS
214
DATA ACCESS TRANSACTION IS A DATA ACCESS STATEMENT AND LIMITING FURTHER COMPRISES IDENTIFYING AT LEAST ONE RULE, ACCORDING TO THE SECURITY POLICY, CORRESPONDING TO THE DATA ACCESS STATEMENT, THE IDENTIFIED RULE RESTRICTING ACCESS TO AT LEAST ONE OF THE DATA ITEMS INDICATED BY THE DATA ACCESS STATEMENT

Fig. 5

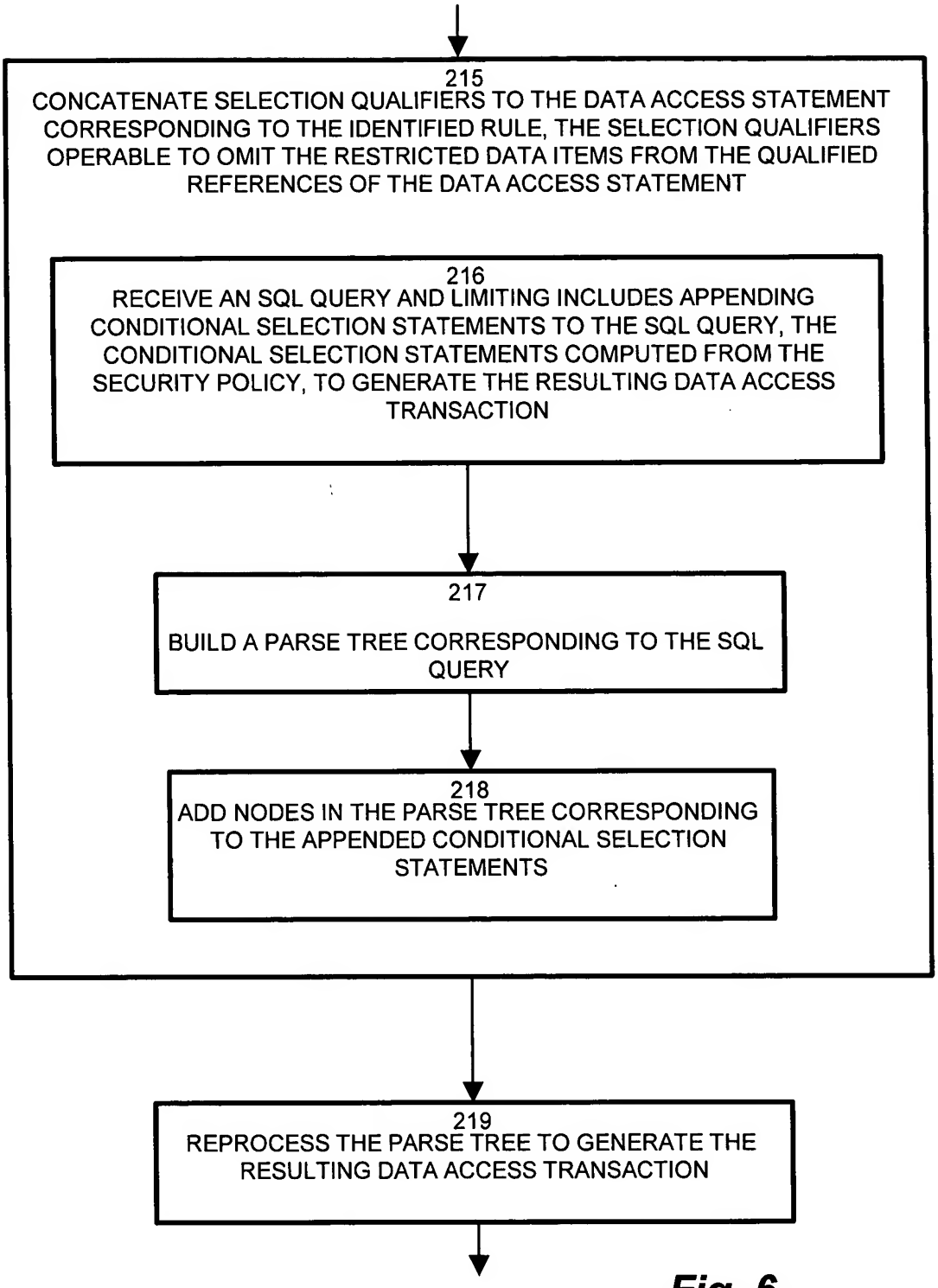

215
CONCATENATE SELECTION QUALIFIERS TO THE DATA ACCESS STATEMENT CORRESPONDING TO THE IDENTIFIED RULE, THE SELECTION QUALIFIERS OPERABLE TO OMIT THE RESTRICTED DATA ITEMS FROM THE QUALIFIED REFERENCES OF THE DATA ACCESS STATEMENT
216
RECEIVE AN SQL QUERY AND LIMITING INCLUDES APPENDING CONDITIONAL SELECTION STATEMENTS TO THE SQL QUERY, THE CONDITIONAL SELECTION STATEMENTS COMPUTED FROM THE SECURITY POLICY, TO GENERATE THE RESULTING DATA ACCESS TRANSACTION
217
BUILD A PARSE TREE CORRESPONDING TO THE SQL QUERY
218
ADD NODES IN THE PARSE TREE CORRESPONDING TO THE APPENDED CONDITIONAL SELECTION STATEMENTS
219
REPROCESS THE PARSE TREE TO GENERATE THE RESULTING DATA ACCESS TRANSACTION

Fig. 6

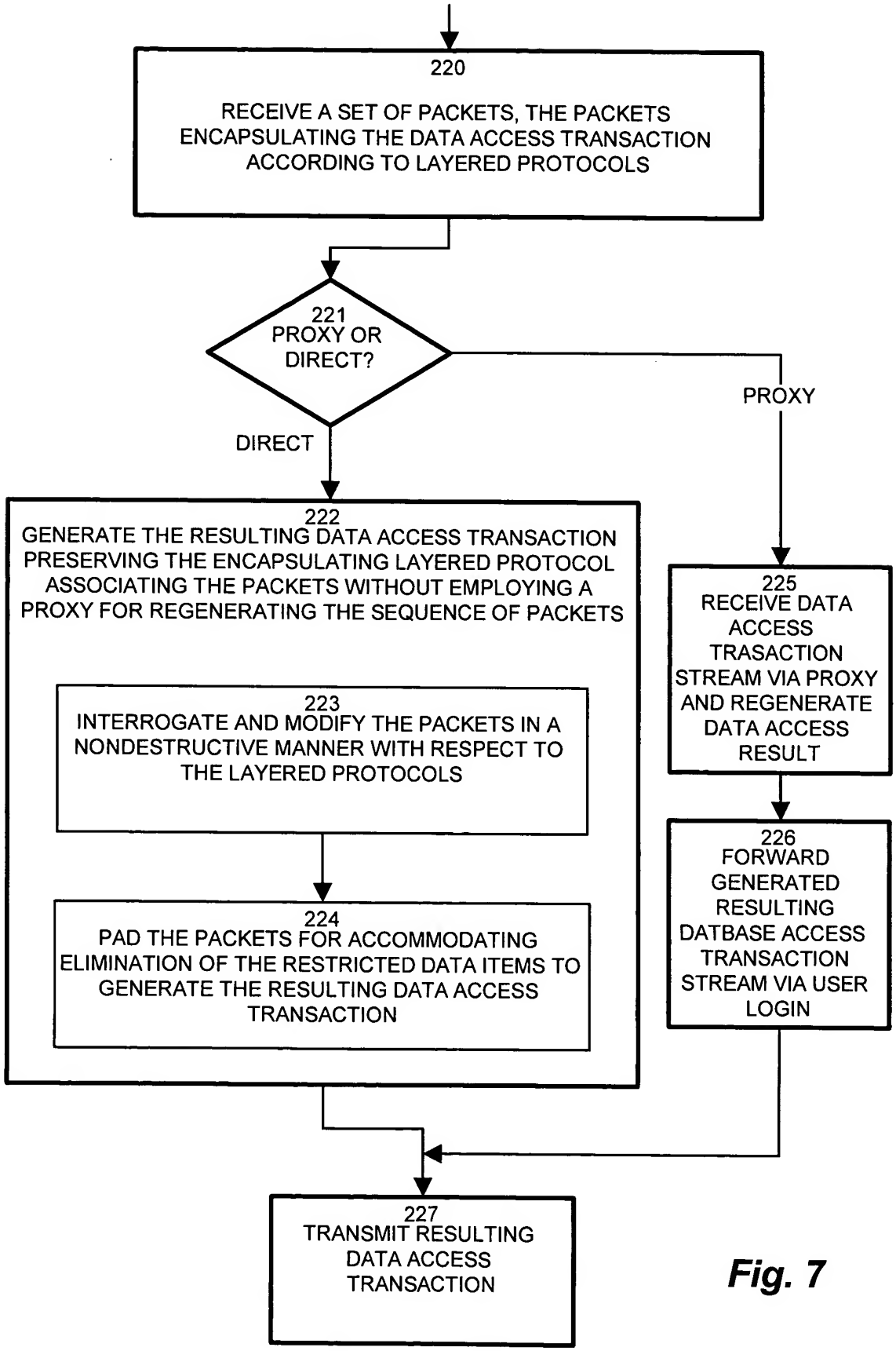

220
RECEIVE A SET OF PACKETS, THE PACKETS ENCAPSULATING THE DATA ACCESS TRANSACTION ACCORDING TO LAYERED PROTOCOLS
221
PROXY OR DIRECT?
PROXY
DIRECT
222
GENERATE THE RESULTING DATA ACCESS TRANSACTION PRESERVING THE ENCAPSULATING LAYERED PROTOCOL ASSOCIATING THE PACKETS WITHOUT EMPLOYING A PROXY FOR REGENERATING THE SEQUENCE OF PACKETS
223
INTERROGATE AND MODIFY THE PACKETS IN A NONDESTRUCTIVE MANNER WITH RESPECT TO THE LAYERED PROTOCOLS
224
PAD THE PACKETS FOR ACCOMMODATING ELIMINATION OF THE RESTRICTED DATA ITEMS TO GENERATE THE RESULTING DATA ACCESS TRANSACTION
225
RECEIVE DATA ACCESS TRASACTION STREAM VIA PROXY AND REGENERATE DATA ACCESS RESULT
226
FORWARD GENERATED RESULTING DATBASE ACCESS TRANSACTION STREAM VIA USER LOGIN
227
TRANSMIT RESULTING DATA ACCESS TRANSACTION

Fig. 7

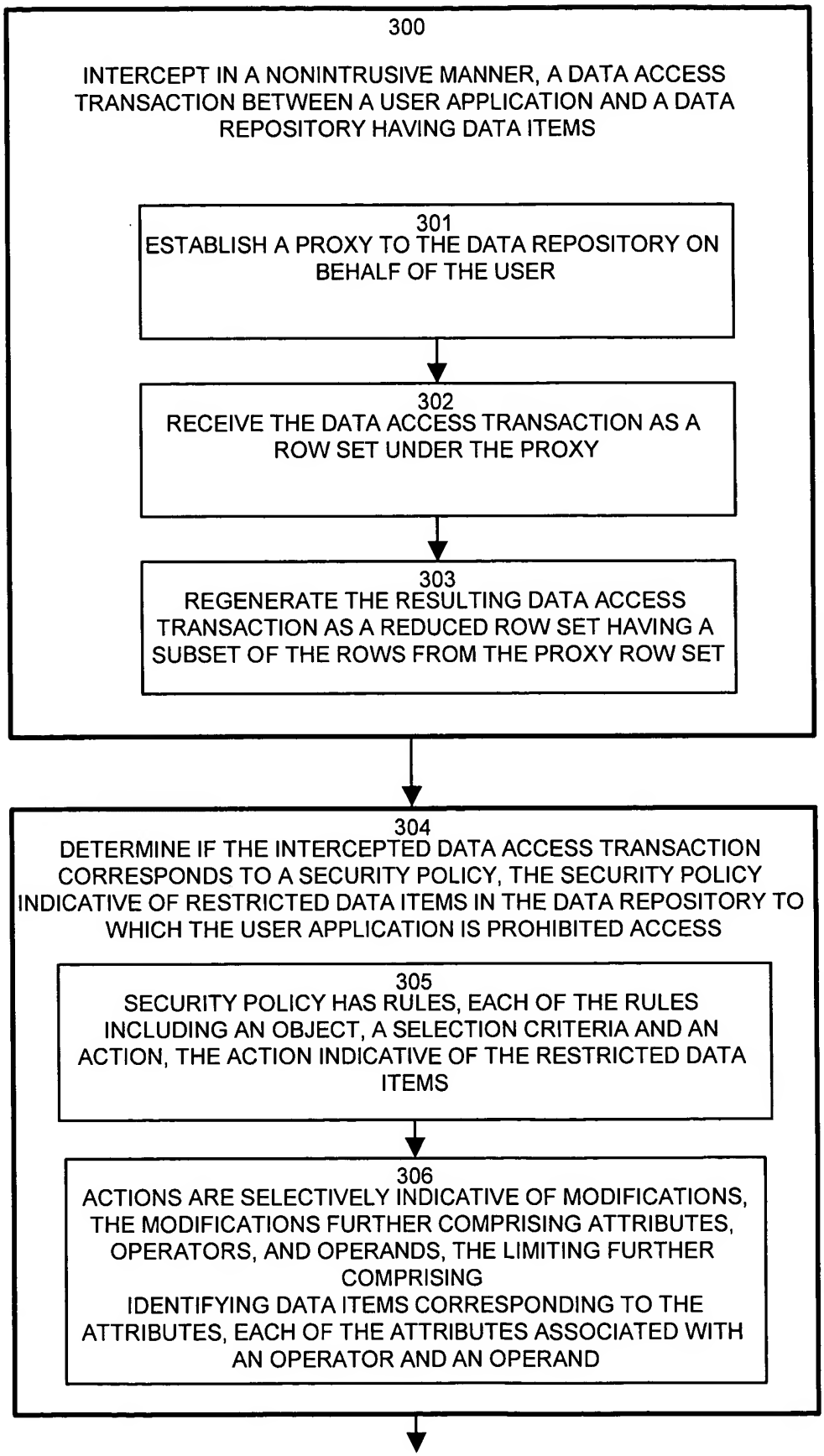

300
INTERCEPT IN A NONINTRUSIVE MANNER, A DATA ACCESS TRANSACTION BETWEEN A USER APPLICATION AND A DATA REPOSITORY HAVING DATA ITEMS
301
ESTABLISH A PROXY TO THE DATA REPOSITORY ON BEHALF OF THE USER
302
RECEIVE THE DATA ACCESS TRANSACTION AS A ROW SET UNDER THE PROXY
303
REGENERATE THE RESULTING DATA ACCESS TRANSACTION AS A REDUCED ROW SET HAVING A SUBSET OF THE ROWS FROM THE PROXY ROW SET
304
DETERMINE IF THE INTERCEPTED DATA ACCESS TRANSACTION CORRESPONDS TO A SECURITY POLICY, THE SECURITY POLICY INDICATIVE OF RESTRICTED DATA ITEMS IN THE DATA REPOSITORY TO WHICH THE USER APPLICATION IS PROHIBITED ACCESS
305
SECURITY POLICY HAS RULES, EACH OF THE RULES INCLUDING AN OBJECT, A SELECTION CRITERIA AND AN ACTION, THE ACTION INDICATIVE OF THE RESTRICTED DATA ITEMS
306
ACTIONS ARE SELECTIVELY INDICATIVE OF MODIFICATIONS, THE MODIFICATIONS FURTHER COMPRISING ATTRIBUTES, OPERATORS, AND OPERANDS, THE LIMITING FURTHER COMPRISING
IDENTIFYING DATA ITEMS CORRESPONDING TO THE ATTRIBUTES, EACH OF THE ATTRIBUTES ASSOCIATED WITH AN OPERATOR AND AN OPERAND

Fig. 8

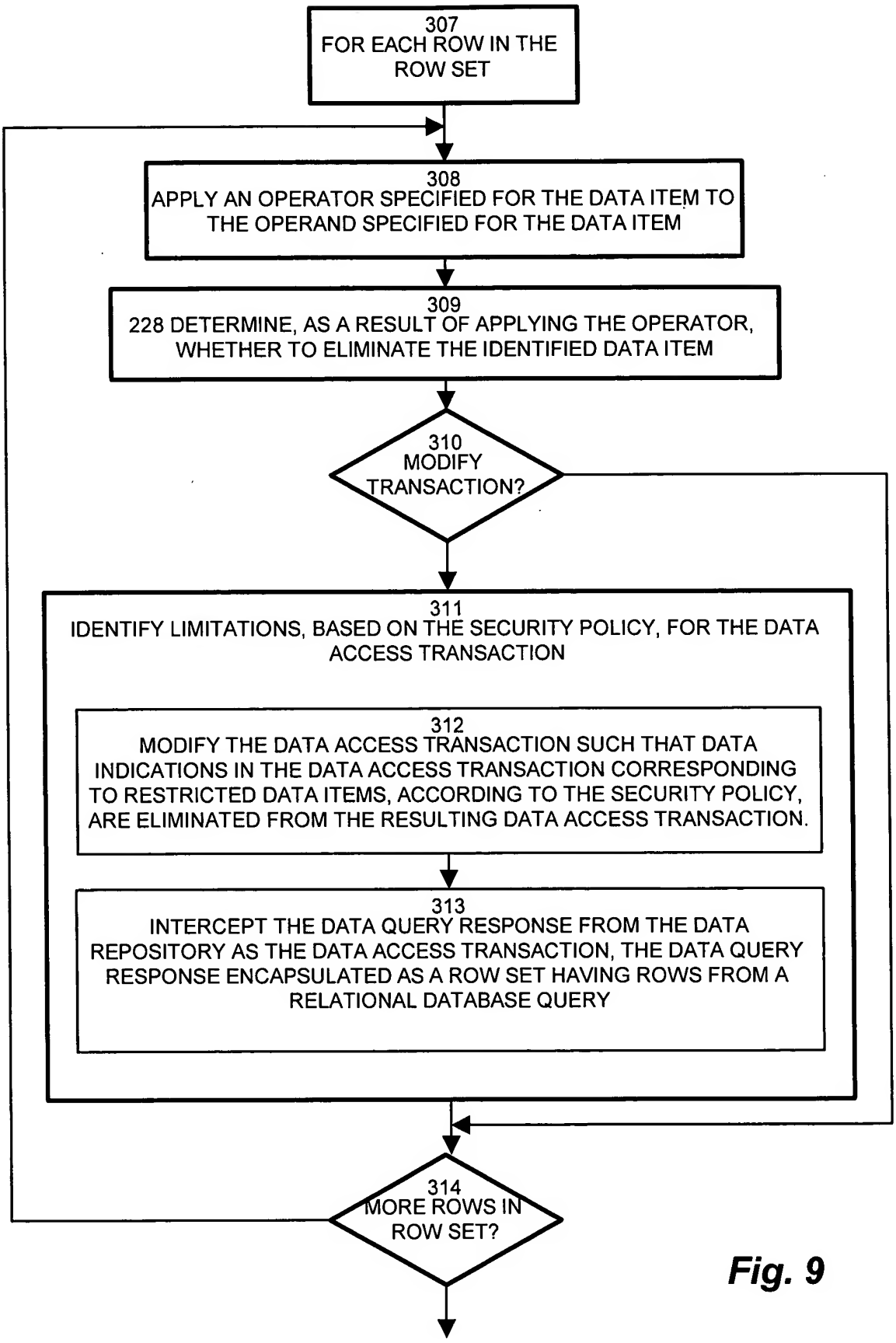

307
FOR EACH ROW IN THE ROW SET
308
APPLY AN OPERATOR SPECIFIED FOR THE DATA ITEM TO THE OPERAND SPECIFIED FOR THE DATA ITEM
309
228 DETERMINE, AS A RESULT OF APPLYING THE OPERATOR, WHETHER TO ELIMINATE THE IDENTIFIED DATA ITEM
310
MODIFY TRANSACTION?
311
IDENTIFY LIMITATIONS, BASED ON THE SECURITY POLICY, FOR THE DATA ACCESS TRANSACTION
312
MODIFY THE DATA ACCESS TRANSACTION SUCH THAT DATA INDICATIONS IN THE DATA ACCESS TRANSACTION CORRESPONDING TO RESTRICTED DATA ITEMS, ACCORDING TO THE SECURITY POLICY, ARE ELIMINATED FROM THE RESULTING DATA ACCESS TRANSACTION.
313
INTERCEPT THE DATA QUERY RESPONSE FROM THE DATA REPOSITORY AS THE DATA ACCESS TRANSACTION, THE DATA QUERY RESPONSE ENCAPSULATED AS A ROW SET HAVING ROWS FROM A RELATIONAL DATABASE QUERY
314
MORE ROWS IN ROW SET?

Fig. 9

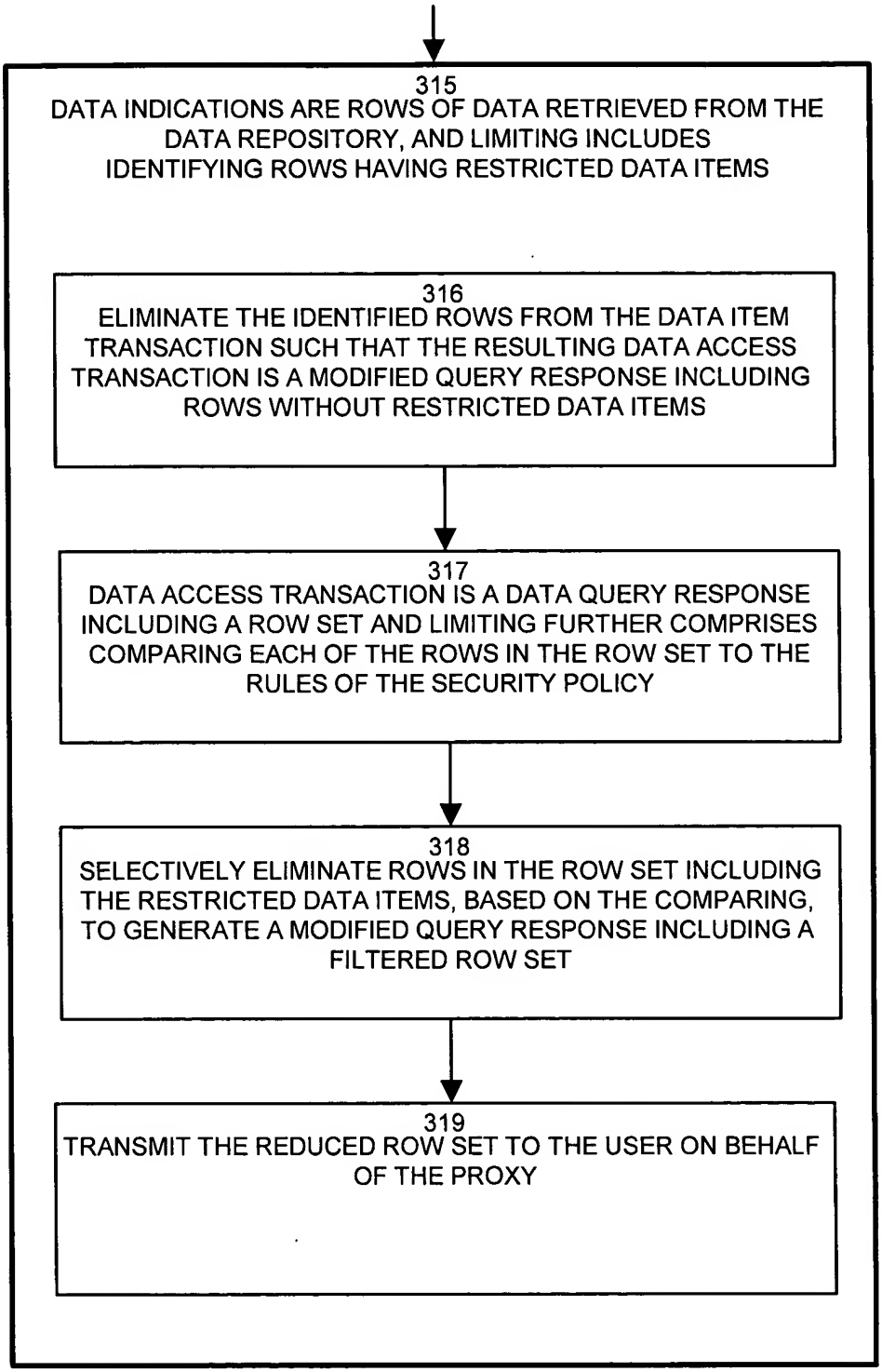
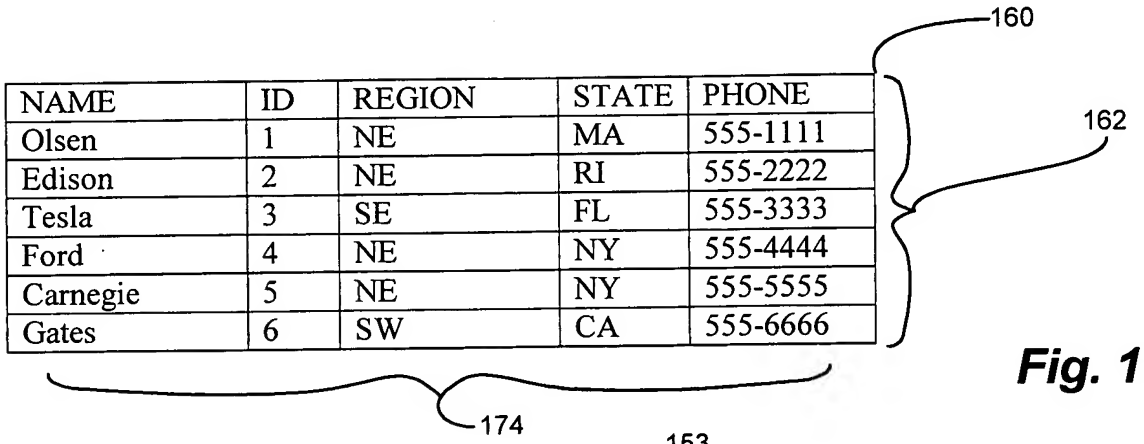
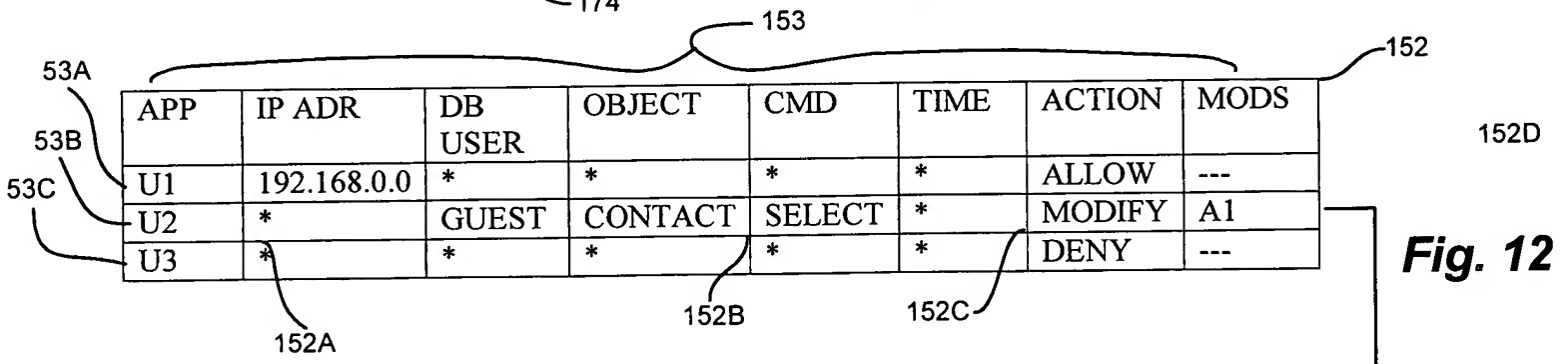

315
DATA INDICATIONS ARE ROWS OF DATA RETRIEVED FROM THE DATA REPOSITORY, AND LIMITING INCLUDES IDENTIFYING ROWS HAVING RESTRICTED DATA ITEMS
316
ELIMINATE THE IDENTIFIED ROWS FROM THE DATA ITEM TRANSACTION SUCH THAT THE RESULTING DATA ACCESS TRANSACTION IS A MODIFIED QUERY RESPONSE INCLUDING ROWS WITHOUT RESTRICTED DATA ITEMS
317
DATA ACCESS TRANSACTION IS A DATA QUERY RESPONSE INCLUDING A ROW SET AND LIMITING FURTHER COMPRISES COMPARING EACH OF THE ROWS IN THE ROW SET TO THE RULES OF THE SECURITY POLICY
318
SELECTIVELY ELIMINATE ROWS IN THE ROW SET INCLUDING THE RESTRICTED DATA ITEMS, BASED ON THE COMPARING, TO GENERATE A MODIFIED QUERY RESPONSE INCLUDING A FILTERED ROW SET
319
TRANSMIT THE REDUCED ROW SET TO THE USER ON BEHALF OF THE PROXY

Fig. 10



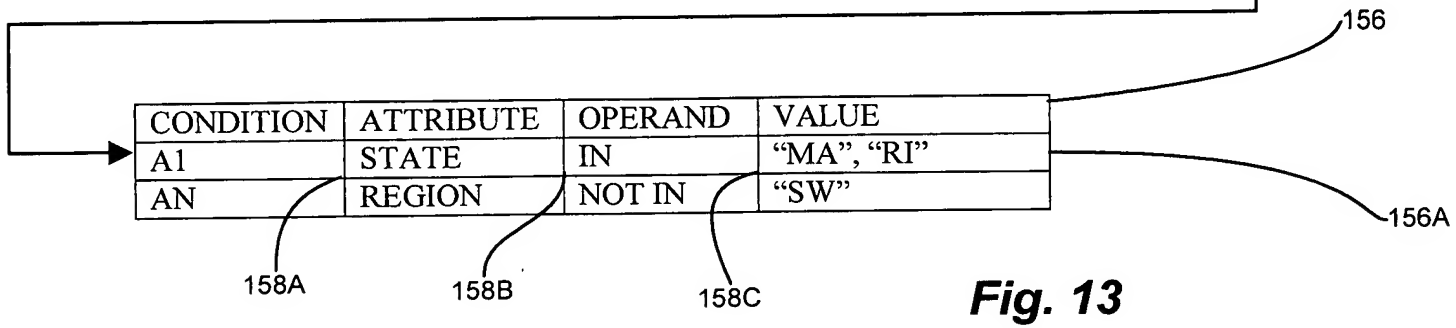
NAME	ID	REGION	STATE	PHONE
Olsen	1	NE	MA	555-1111
Edison	2	NE	RI	555-2222
Tesla	3	SE	FL	555-3333
Ford	4	NE	NY	555-4444
Carnegie	5	NE	NY	555-5555
Gates	6	SW	CA	555-6666

Fig. 11



APP	IP ADR	DB USER	OBJECT	CMD	TIME	ACTION	MODS
U1	192.168.0.0	*	*	*	*	ALLOW	---
U2	*	GUEST	CONTACT	SELECT	*	MODIFY	A1
U3	*	*	*	*	*	DENY	---

Fig. 12



CONDITION	ATTRIBUTE	OPERAND	VALUE
A1	STATE	IN	"MA", "RI"
AN	REGION	NOT IN	"SW"

Fig. 13

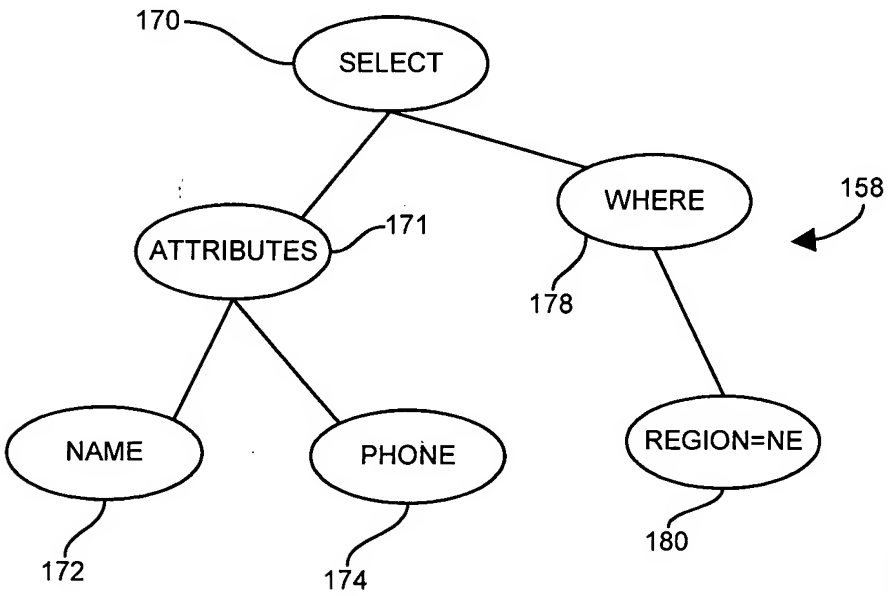


Fig. 14A

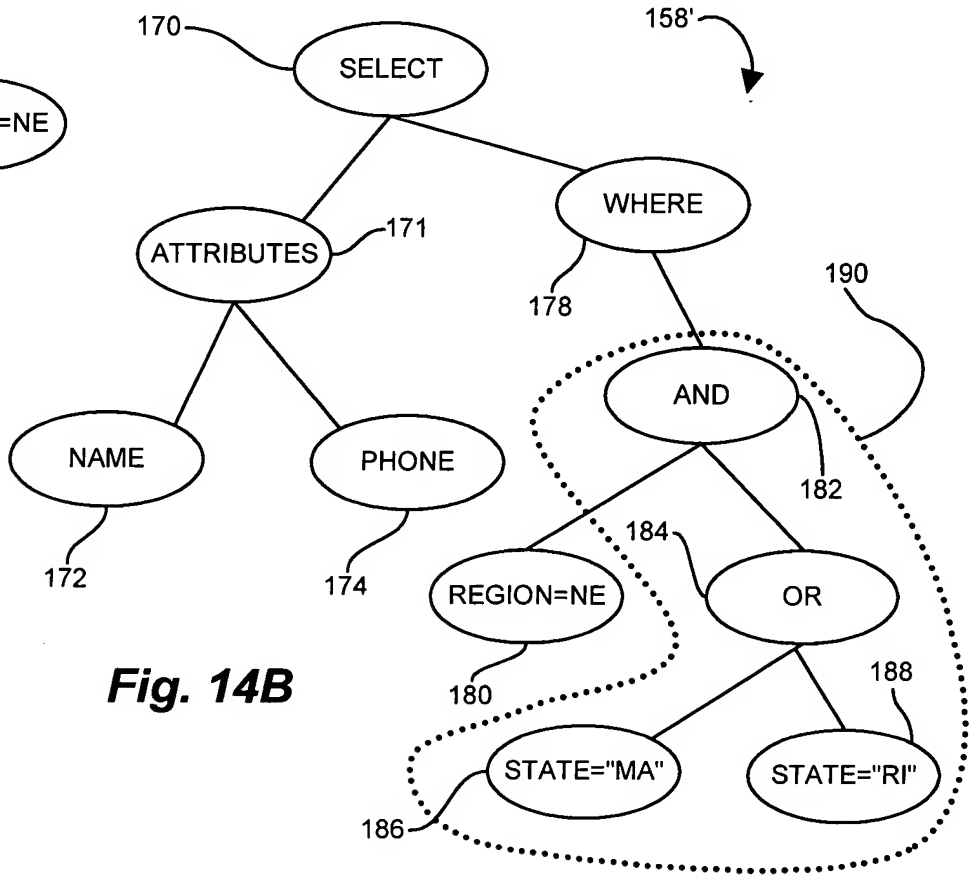


Fig. 14B